BayRS Version 12.02 and Site Manager Software Version 6.02 Release Notes

BayRS Version 12.02
Site Manager Software Version 6.02

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

AN, BLN, GAME, and Bay Networks are registered trademarks and ARN, BayRS, and the Bay Networks logo are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Technical Support

Bay Networks Technical Publications vii
Bay Networks Customer Service vii
How to Get Help viii
Bay Networks Educational Services viii

BayRS Version 12.02 and Site Manager Software Version 6.02 Release Notes

Maintenance Release Methodology 1
Year 2000 Compliance 2
Image Builder Operational Note 2
PC Site Manager READ ME FIRST File 2
Known Anomalies in Version 12.02/6.02 5
BayRS Version 12.02 Fixed Anomalies 6
Site Manager Software Version 6.02 Fixed Anomalies 37

Technical Support

Bay Networks Technical Publications

You can now print technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs*. Find the Bay Networks products for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

Documentation sets and CDs are available through your local Bay Networks sales office or account representative.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Bay Networks Educational Services

Through Bay Networks Educational Services, you can attend classes and purchase CDs, videos, and computer-based training programs about Bay Networks products. Training programs can take place at your site or at a Bay Networks location. For more information about training programs, call one of the following numbers:

Region	Telephone number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 282 when prompted 978-916-3460 (direct)
Europe, Middle East, and Africa	33-4-92-96-15-83
Asia/Pacific	61-2-9927-8822
Tokyo and Japan	81-3-5402-7041

BayRS Version 12.02 and Site Manager Software Version 6.02 Release Notes

This document lists the anomalies (also referred to as bugs, change requests, or CRs) that have been fixed in Bay Networks® BayRS™ Version 12.02 and Site Manager Software Version 6.02. BayRS Version 12.02 includes all anomalies that were fixed in 12.01 Revisions 1, 2, and 3; Site Manager Software Version 6.02 includes all anomalies that were fixed in 6.01 Revisions 1 and 3.

Use the BayRS Version 12.00 and Site Manager Software Version 6.00 documentation with BayRS Version 12.02 and Site Manager Software Version 6.02.

Maintenance Release Methodology

BayRS Version 12.02 and Site Manager Software Version 6.02 are Maintenance Releases.

Bay Networks is introducing a new methodology for releasing Bay Networks routing software.

Maintenance Releases are designated by a change in the second number to the right of the decimal point. They provide a collection of software bug fixes for the current Major Release. No new software or hardware features or functionality for either software or hardware is introduced beyond that already contained in the current Major Release.

A Maintenance Release will occur approximately each 3 to 4 months after a Major Release occurs. A Maintenance Release replaces the current Major Release (or the prior Maintenance Release) on the Price List and will become the current shipping version of BayRS. Each Maintenance Release will be a consolidation of the prior bug fixes made through Revision Releases, and will roll up all such software bug fixes provided by the recent Revision Releases.

Year 2000 Compliance

BayRS Version 12.02 and Site Manager Software Version 6.02 are Year 2000 Compliance Certified by Bay Networks. They have successfully passed Bay Networks Test Procedure which tests conformance to Bay Networks Year 2000 compliance definition, both of which can be found at Bay Networks Year 2000 Web Site at *http://www.baynetworks.com/year2000/*.

Image Builder Operational Note

If you are using Image Builder in Site Manager Software Version 6.10 to modify a BayRS Version 12.02 router image, you will receive an error. Please contact Bay Networks Customer Support to obtain the patch for this problem.

PC Site Manager READ ME FIRST File

The contents of the PC Site Manager READ ME FIRST file are unreadable. The complete text appears below:

```
/*=====================================================*/
/*            PC/Site Manager 6.02 */
/*            README FILE */
/*            Bay Networks, Inc. */

/*            Copyright 1988-1998. All Rights Reserved.  */
/*=====================================================*/

/*============================*/
---- SYSTEM REQUIREMENTS ----
/*============================*/

486 PC (Pentium recommended)
```

Microsoft Windows 95
16 MB of RAM (minimum)
60 MB of free disk space
Microsoft Windows 95 TCP/IP protocol
and compatible network adapter and driver.
CD-ROM drive
VGA monitor (SuperVGA monitor recommended)

/*=========================*/
---- BEFORE YOU BEGIN ----
/*=========================*/

1. Manager Version 6.02 requires the
Windows 95 TCP/IP protocol stack and a
compatible network adapter and driver.

If you purchased a machine with Windows 95 and
a network adapter installed, most likely you
have the correct TCP/IP protocol, network
adapter, and driver. Proceed to step 2
to test TCP/IP.

However, if your PC was upgraded from Windows
3.1, it may have an existing 16 bit TCP/IP
stack like Distinct TCP/IP Run Time. In this
case, you must uninstall the 16-bit TCP/IP
stack before adding the Windows 95 TCP/IP
protocol stack.

To uninstall a 16 bit TCP/IP stacks, refer to
the TCP/IP provider's documentation and
support for help in removing the stack's path
statements, services file, and WINSOCK.DLL
files dated prior to 7/11/95. (That is the
date of the WINSOCK.DLL file installed by
Windows 95.)

To add or update a protocol, network adapter,
or driver, refer to the appropriate
documentation and support from Microsoft and
the adapter manufacturer. Protocols and driver

updates are added from the Network option of the Control Panel. New network adapters and their drivers are added from the Add New Hardware option of the Control Panel.

Windows 95 attempts to match a driver to the network adapter installed on your computer. If Windows 95 cannot match a compatible driver, you need to update the drivers. Contact the adapter manufacturer for the latest drivers. Microsoft and other Windows 95 Web sites may also have updated drivers.

Refer to "Microsoft Windows 95 Resource Kit" for additional technical information about these issues. A hard copy is available from Microsoft Press.

2. Test the TCP/IP installation by pinging an IP address. If you are unable to PING the adddress, there could be a problem with the TCP/IP installation

/*====================*/
--- Installation ---
/*====================*/

To install the PC/Site Manager software from CD:

1. Access the Run window by selecting Run from the Start menu.

2. Type the CD-ROM drive, path, and executable file:
<CD-ROM drive>:\ms_win\setup.exe
The D: drive is usually the CD-ROM drive.

3. Click on OK.

/*=========================*/
---- Troubleshooting -----
/*=========================*/

GENERAL:
========
(Problem) - No text is displayed on some or all of the screens.
(Solution) - Make sure that the jam.ini file
is in the WINDOWS directory.
For Example: c:\windows\jam.ini

Known Anomalies in Version 12.02/6.02

This section describes the following known anomalies:

CR 74897: IP.

When creating a static route (e.g., 128.10.8.0/255.255.255.0/1), the router erroneously generates the following error message in the router log file:

```
#  2: 04/16/98 09:44:24.096   WARNING   SLOT  5  IP     Code: 56

Error when configuring status route 128.10.8.0/255.255.255.0/1
```

In this case, the log file falsely indicates a problem with the creation of the static route when in fact the static route is created.

CR 81714: X.25.

You may see an Orphaned Buffer error during heavy IPEX traffic containing varying packet sizes. This error was recorded once in BayRS 12.02 and the data sessions all recovered.

CR 81761: DVMRP.

When you configure DVMRP in dynamic mode, Site Manager attemps to set the wfDvmrpBase.18.0 MIB attribute, which results in an SNMP set error message. This prevents you from properly configuring DVMRP.

BayRS Version 12.02 Fixed Anomalies

Bay Networks has fixed the following anomalies in BayRS Version 12.02.

==========

SITE MANAGER COMPATIBILITY

==========

Router Version is managed by Site Manager version

v12.02 ----------> 6.02

v12.01 revision 1 ----------> 6.01 and 6.01 rev 1

v12.01 revision 2 ----------> 6.01 and 6.01 rev 1

v12.01 revision 3 ----------> 6.01 and 6.01 rev 3

==========

CR 80180: DLSw.

A problem may occur when you try to establish DLSw TCP peers. If you notice only the write (2067) to read (2065) TCP connection being opened for RFC 1434 and 1795 types of peers, and you see that connection establishment between the client and host takes a long time, set this mib value from the Technician Interface:

s wfDlsPeerEntry.wfDlsPeerInteroperability 2;commit

This is only applicable on routers running 11.03/rev/3 or above, or 12.01/rev/1 or above with DLSw peers configured.

CR 73533: IPEX/X.25 Gateway.

When IPEX/X.25 Gateway is run with header type NONE (No Boundary protocol), messages may be dropped by IPEX as they are sent to the TCP subsystem for transmit.

CR 80105: ATM.

In SSCOP, when the top of the transmit window is reached, subsequent messages are queued up for later. When the transmit window is incremented, the postponed messages are not sent out. The messages remain in the private buffer pool for the SSCOP gate until some event (e.g., bouncing signaling) restores them. Depending on the circumstances, the slot may run out of buffers.

CR 80231: FireWall.

The router reports invalid interface numbers to Firewall's Logviewer. Instead of reporting the circuit number, the router reports the line number.

CR 80007: TCP.

TCP peers are very slow to form in a DLSw environment where many peers are configured.

CR 33841: ATM.

The SSCOP window does not conform to the Q.SAAL (Q.2110) specification. Bay Networks router code does not respect the Q.SAAL window credit specified by the switch. As a side effect of this change, LECs may struggle to come up if signaling goes down for any reason because the router and the switch cannot communicate fast enough to keep the connections from timing out. If this occurs, we suggest that the value of wfAtmSscopEntry.wfAtmSscopMaxPd be set to a low value (4 or 5).

CR 80212: IPEX/X.25 Gateway.

IPEX Gateway sessions may hang under heavy load of large packets.

CR 80772: IPEX/X.25 Gateway.

If the IPEX State machine in the established (EST) state receives a reset request, it stays in the established state and never goes to the connection (CONN) state.

CR 80532: BGP.

Routes are not properly withdrawn if a BGP route matches a network criteria exactly.

CR 30189: Scripts.

If you run the embedded **show** script for an IP circuit whose circuit name contains a lowercase alpha character, the circuit is not found.

CR 33681: LNM.

When you run the file *lnm.bat*, it loops infinitely.

CR 70923: DECnet.

In a simple DECnet environment, an adjacency is being removed from the wfivLevel1RouteEntry attribute prematurely because the router incorrectly counts 3 Hello packets as received.

CR 72633: VINES.

When a VINES client sends a broadcast request, all servers respond. The client connects to the first server and then sends a disconnect message to the other servers. When the VINES client sends the disconnect message, the VINES interface on the router performs intensive processing for the forward cache and the slot where the client resides experiences a Watchdog fault.

CR 73793: DLSw.

If the upstream/host side issues a disconnect followed by an XID poll 5 ms later, the XID poll will reset the internal LLC connection from stat HALT_PENDING to CIRCUIT_PENDING. The SDLC side disconnects, while the LLC side proceeds to the connected state. This condition results in an interoperation problem with the 5745 Enterprise Server.

CR 74752: NAT.

A problem exists when running NAT with the Mapping Entry timeout enabled. If you have set a large amount of dynamic mapping entries and set the Max Timeout value, the router faults with a tag violation.

CR 75084: IP.

A problem exists in an ISP environment in which full internet routes are installed (50000). Attempting to run an SNMP "get" of the arp table (wfIpNetToMediaEntry) causes MIB_MGR to consume CPU from 259 ms to 305 ms multiple times. This causes forwarding performance problems on interfaces related to the slot where the "get" is being executed.

CR 75429: IP.

When a router running in ISP mode receives an all subnet broadcast (ASB - traffic whose destination includes other interfaces on the same router) a bus error occurs.

CR 26774: ATM.

A router running LANE crashes with an MCP error after losing and then regaining signaling.

CR 32385: APPN.

Dynamically adding LS to a frame relay interface causes a bus error to occur on the router.

CR 34175: ATM.

An MCP error occurs during a dynamic configuration in an Ethernet LANE environment while adding IP/RIP to the second service record.

CR 34236: SYNC.

A bus error occurs when trying to use asynchronous PPP with a Hayes modem.

CR 34595: Router Redundancy.

If you configure one router interface for router redundancy, the router checks only the first resource in the Router Redundancy Resource List for its availability via pings.

CR 34991: Firewall-2.

FireWall performance degradation occurs as a result of a leakage fix that existed in phase 1. Performance suffers between 10% and 90% with a packet size of 64 bytes. These numbers improve when the packet size is increased.

CR 35096: SDLC.

The SDLC code does not properly interoperate with the AS/400 high-speed line controller with respect to flag streaming.

CR 35704: QLLC.

When a QLLC/X25 end station receives a QUA in response to sending out a QDISC, it is possible that the end station will not clear the X.25 call. This causes the QLLC connection to not re-establish because the QLLC router side expected the receiver of the QUA to clear the call.

CR 35739: IGMP.

When attempting to create 125 source group pairs, some of the source group pairs do not have an outbound slot.

CR 35985: SDLC/DLSw.

A DLSw connection does not properly recover after bringing down the SDLC line during flow control.

CR 71175: Switched Services.

If you have backup circuits configured, setting the schedule parameter to any valid value has no functional effect. When the primary circuit fails, the backup circuit is activated, regardless of the configured time/day. This occurs only when the Availability Mode parameter is set to Not Available.

CR 71429: IP.

A router running in ISP mode may experience a bus error when a forward-to-next-hop filter is matched and the next hop does not exist and there is no route to the final destination of the frame.

CR 71769: Source Route Bridge.

In IP Encaps, source route frames received on a source routing interface do not get sent out over the IP Encaps cloud after IP is restarted.

CR 72190: IGMP.

This is an enhancement request to add a MIB attribute to control whether non-local reports should be accepted.

CR 72328: IP.

When adding IP to a 10 MB Ethernet interface, the router faults.

CR 72641: NAT.

If both the local host address and the translated address contain two digits at the end, FTP fails when you issue a **port** command. For example, if the local host IP address is *xx.xx.xx.*16, and the translated address is *xx.xx.xx.*17, an FTP session can be initiated. However, as soon as you issue a **port** command, the FTP session terminates.

CR 73832: SDLC.

The router fails to set the poll bit in I-frames on an SDLC line, which can result in excessive retransmissions and line performance degradation with certain controllers.

CR 74090: QLLC.

The router is unable to establish a session between the IBM 3174 X.25 client and an IBM Token Ring host in a "Downstream QLLC Network". The router generates an error in *buf_float.c* at line 113.

CR 74946: X.25.

An X.25/PTOP circuit may remain operational in the UP state after powering off either a modem-eliminator or a CSU/DSU device connected to the port.

CR 74977: IPEX/X.25 Gateway.

IPEX Gateway Mode fails to keep track of whether it reports the PVC in a down state, or its peer reports the PVC as down. Rather, it accepts TCP opens even when the X.25 PVC is down, preventing X.25 from transmitting packets properly.

CR 74991: IPEX/X.25 Gateway.

When IPEX is in gateway mode and the TCP side of an IPEX session terminates, it resets the X.25 side and then re-establishes the TCP session. But under heavy load, the TCP session can be reestablished before X.25 has completed its reset, causing synchronization problems between the two sides of the IPEX session.

CR 74993: IPEX/X.25 Gateway.

IPEX in gateway mode does not send Reset 1d if the server side router's TCP open fails. After booting both routers, and if the server is down when the client attempts to establish an IPEX session, the server side router should send a Reset 1d to the client side router to notify the client that the IPEX session failed. The log files shows that IPEX sent a reset message to X.25, but X.25 failed to transmit it because X.25 was not in a data transfer state.

CR 75519: QOSPF.

Non-self-generated QOSPF Resource Reservation Advertisements (RRA) and Deterministic ABR-Advertisements (DABRA) received from a neighbor were not flooded out to other neighbors, causing the route-pinning feature to fail.

CR 75484: DLSw.

During certain protocol exchanges, DLSw connections can get stuck in CIRCUIT_PENDING and fail to recover until you reset DLSw or LLC (or reboot the router).

CR 33106: MOSPF.

The router experiences a tag violation error, causing it to fault under heavy traffic.

CR 33530: Telnet.

When there are many dynamic environment variables defined, an outbound TELNET session hangs and freezes the entire Technician Interface session.

CR 34511: Translation Bridge.

Configuring translation bridge (XB) dynamically over TR LANE causes an Exception Vector 2 MCP error to occur on an ARE processor module.

CR 35570: PPP.

The IPX maximum frame size for a PPP link is calculated to be 4 bytes less than its required value.

CR 36062: DLSw.

An orphan buffer occurs when a DLSw connection is terminated.

CR 71025: DLSw.

DLSw causes an orphan buffer over ARE in DLSw version 1795 environment. The DLSw peer is also running RFC 1795.

CR 71423: QLLC.

A DLSw connection receives CANUREACH, but will not generate an X.25 call to the adjacent host.

CR 71517: IPX.

An IPX Static Route is not properly installed in the router's IPX route table.

CR 71975: DLSw.

The DLSw connection fails to recover after the granted units counter reaches zero, which is a protocol violation.

CR 72792: LLC.

When an LLC interface is disabled, a panic may occur after 30 minutes instead of after one minute if the router is having resource problems.

CR 28639: APPN.

To use a default DLUS name for link stations that are not defined in the APPN Adjacnet Link Stations table, you must define both the Default DLUS name and the Backup Default DLUS name.

CR 31110: SNMP.

When you type **show snmp base** using the Technician Interface, the displayed information has some misspelled words.

CR 32728: APPN.

If you enable APPN on a HSSI interface configured for SMDS, the router experiences a bus error.

CR 32804: Learning Bridge.

This is an enhancement request to add a MIB attribute under wfBrTp called wfBrTpBaseFDBPortChange, which counts the number of times that an entry in the forwarding table has changed ports (that is, a MAC address is learned via port A, then re-learned via port B).

CR 33900: TCP.

The current TCP code does not have the capability to deregister on the slots on which it has registered the connection. Rather, it tries to deregister on all the slots passed in by the client when the connection was opened.

CR 35181: MCE1.

The ASN router experiences a tag violation upon bootup when MCE1 is not physically present (although configured).

CR 35497: MOSPF.

A bus error occurred on a router configured with 1000 source group pairs and generating multicast traffic at a rate of 14,000 packets per second.

CR 35770: DVMRP.

A router receiving traffic at a rate of 10,000 packets per second for 2000 source groups experiences a watchdog error and subsequently faults.

CR 35940: DVMRP.

The router experiences a panic at *dvmrp_cache.c* at line 443.

CR 72024: FTP.

A problem occurs when attempting to transfer small files from a UNIX system to the router via FTP.

CR 72146: OSI.

When you alter the cost of an OSI External Adjacency, the new cost is not reflected in the routing table until you restart the adjacency, interface, or OSI.

CR 72151: OSI.

When the router updates an OSI interface Hello password, the new security string is not reflected in the router's Hello messages until you restart either the interface or OSI.

CR 72237: IP.

When you reinitialize BootP after restarting an ATM interface, a machine check occurs in BootP.

CR 72565: Switched Services.

You cannot manually activate a standby circuit.

CR 72996: Switched Services.

SPID is not registering after TE1 loss because two SPIDS are sent out of order.

CR 73254: DVMRP.

wfDvmrpBasePolicyEnable should be obsoleted from the wfDvmrpBase record.

CR 75414: APPN.

In a large APPN network, some routers fault at unpredictable times.

CR 75456: APPN.

An intermittent bus error occurs when an APPN link to an RS/6000 configured as an NN goes down.

CR 75726: Switched Services.

The weekend schedule for a backup circuit does not function correctly when another schedule is configured. For example, if you modify the date on the router so that the backup circuit is active for the scheduled weekday, the backup circuit is not active.

CR 29307: APPN.

When you have Dependent (PU2.0) devices in session and enter the command **appn show dlur route**, invalid data is displayed in the route field.

CR 71585: Technician Interface.

The Technician Interface command **show csmacd stats** displays large numbers (approaching 2,000,000,000) as negative numbers.

CR 33867/34692: IP.

IP Packet fragmentation in ISP mode is not working properly.

CR 33685: OSI.

Duplicated OSI routing table entries may occur when load balancing is disabled.

CR 72134: ASN.

An ASN router with 100 MB Ethernet modules and Circuitless IP experiences bus errors at bootup.

CR 71001: ARN.

The LEDs remain on for both B channels even though both channels are not being used.

CR 78426: Learning Bridge.

An orphan buffer may occur when you bridge packets over a PPP interface.

CR 78501: DLSw.

DLSw does not handle the HALT_NOACK command defined in RFC 1795.

CR 78498: GAME.

No log message is written when a fault occurs on the router and no crash dump is written to the flash.

CR 33969: OSI.

Disabling the OSI interface will cause a fault in *mib_ent.c* on another OSI slot.

CR 74815: ATM.

A watchdog error may occur when you process LE_ARPs on an ATM interface.

CR 72794: Technician Interface.

Disabling a multiline/multilink circuit group via the script **disable sync circuit** *<cct name>* does not disable the entire group. This command disables only the first circuit configured in this bundle; subsequently, you must disable the other lines manually.

CR 74301: Technician Interface.

Log and dir displays show year as only 2 digits; should display as 4 digits.

CR 75352: NAT.

NAT stops translating traffic from the global port to the local port for random dynamic mappings. Instead, ICMP redirects are transmitted out the global port.

CR 76040: WCP.

Bouncing a Frame Relay PVC that has WCP enabled may cause a bus error.

CR 78737: SDLC.

An SDLC link configured as primary multi-drop fails to respond after receiving an I-Frame with the poll bit set. If there are 2 PUs, one of them must be inactive on the host for this condition to occur. The router should send either another I-Frame or RR.

CR 78787: IPEX.

IPEX (Gateway) does not respond to the Reset Request Cause=0 and Diag=0.

CR 26530: MIB.

The MIB-II variable ifEntry reports incorrect information for ifOperStatus for a redundant interface.

CR 75239/78321: BGP.

When you have more than one BGP peer between a pair of routers, and you have BGP collision detect disabled, changes to the announce policy do not take effect.

CR 78421: ATM.

A router running Source Route Bridge over Token Ring may cause an MCP error.

CR 78669: DLSw.

Slow performance occurs when you transfer NetBIOS files using DLSw RFC 1795.

CR 33696: Frame Relay Switch.

When you change secondary (Host FRAD) point-to-point or multidrop local device DLSw mode to primary while operating in dynamic configuration mode, all sessions on the slot drop.

CR 74486: BGP.

The BGP peer delay parameter should not be configurable through the BCC. The BCC is able to configure more BGP peer-configurable parameters than Site Manager. Site Manager cannot configure the delay or detect-as-loop parameters.

CR 71942: FTP.

The router crashes when you try to change the local directories while the router is connecting.

CR 78499: SDLC.

SDLC trace logging is not fully implemented.

CR 79286: Router Redundancy.

The router redundancy script **show rredund role** displays the role incorrectly; it displays both the members as primary under certain conditions.

CR 73045: ARE.

An ARE may intermittently hang or have out-of-buffer crashes due to buffers getting stuck in a "holding tank."

CR 73435: ISP.

Multicast traffic is not forwarded when ISP mode is enabled.

CR 74931: ATM.

An ATM interface stops transmitting or intermittently transmits if a router is connected to an ATM switch that supports OAM. This problem occurs if the remote end of a PVC is brought down.

CR 33600/28218: IP.

A fault occurs after a route with an invalid subnet mask is added to the route table and then a subsequent route in the same range is submitted.

CR 34487: PPP.

If you have multiple PPP circuits on the same slot configured for LQR, a race condition may occur when the circuit states change, causing a bus error.

CR 35021: OSPF.

The ignore action of an OSPF accept policy does not work.

CR 71691: IP.

This is an enhancement request to add support for Multicast Packet Replicator (MPR).

CR 73764/73480: IP.

The router drops IP packets after ARPing for a destination address.

CR 32997: IP.

When a Token Ring interface receives a segmented IP packet that was incorrectly routed to it, the interface fails to send a second packet to the next correct hop.

CR 36033: IP.

Issuing the **traceroute** command with the **LSRR (-g)** option causes a packet that arrived with a ttl of 1 to have a ttl of 255.

CR 30447: BGP4.

This is an enhancement to optimize regular expression processing for BGP4 route policies.

CR 29419: IP.

This is an enhancement request for a router in host-only mode (configured as Bridge) to listen to RIP packets so that it can make forwarding decisions for self-generated IP traffic.

CR 21299: APPN.

APPN parameters wfAppnNodePortMaxRcvBtuSize, wfAppnNodePortMaxSendBtuSize in wfAppnNodePortEntry, and wfAppnNodeLsMaxSendBtuSize in wfAppnNodeLsEntry need to be changed from 2057 to 1500 to accommodate the 1600 MTU size of a WAN port.

CR 23552: Switched Services.

If a dial-on-demand circuit is active in standby mode, and you disconnect and then reconnect the BRI line, the standby circuit connection is not properly reestablished.

CR 24390: ATM.

An MCP may occur after you dynamically change a Hybrid Mode PVC on an ATM interface.

CR 27324: ISDN.

This is an enhancement request to allow you to configure the number of times a router will attempt to register a SPID (for basic rate ISDN) with an ISDN switch.

The following parameters were added to wfIsdnLocalPhoneNumEntry: wfIsdnSpidRetries, wfIsdnSpidRetryAttempts, wfIsdnSpidRetryTimer, and wfIsdnSpidResetBri.

CR 27745: DLSw.

When you reset an IP interface on a DLSw router, a bus error occurs.

CR 28088: IPX.

For IPX Route Filters, the log message `IPX Route Filter with rule number 1 includes rule number 2 on circ. index 1` is generated despite the fact that the filters are configured correctly.

CR 28250: FTP.

When you transfer a file with a file name that starts with a numeric value to the router, the router faults and receives orphan buffers.

CR 28589: BootP.

If you configure DHCP on a multinetted interface, the last IP address configured should become the DHCP gateway. If you reboot the router, the last configured IP address is no longer the DHCP gateway. Instead, another IP address on that interface becomes the gateway.

CR 29517: IPX.

If a router receives an IPX SAP packet on an interface with a network number that is different from the one for which the packet is destined, the packet is not dropped.

CR 29813: ARP.

Routers fail to update the ARP table according to specifications in RFC 826.

CR 30380: ATM.

An MCP error occurs when you disable and enable ATM signaling entities.

CR 30440: ISDN.

After you reset an ISDN BRI interface using the Technician Interface, SPIDs get rejected.

CR 30591: DLSw.

There is no mechanism to display and monitor DLS and LLC2 connections on a per-slot and per-interface basis.

The following four MIB attributes were added:

wfDlsSlotCurrentSessions displays the number of DLSw connections on the slot that are in a CONNECTED state. wfDlsSlotHiWaterSessions displays the maximum value reached by wfDlsSLotCurrentSessions since DLSw was enabled, or since wfDlsSlotHiWaterReset was set to 2. wfLlcInterfaceCurrentLinks displays the number of links on the LLC interface. wfLlcInterfaceHiWaterLinks displays the maximum value reached by wfLlcInterfaceCurrentLinks since the LLC base was enabled, or since wfLlcInterfaceHiWaterReset was set to 2.

CR 30870: ISDN.

When you change a valid ISDN local telephone number in dynamic mode, the router terminates operation.

CR 30998: DLSw.

If you substitute a wildcard as part of a MIB instance ID when performing a MIB get operation on the MIB entry wfDlsConnectionEntry, the router responds with an incorrect answer.

CR 31797: ARP.

This is an enhancement request to add a Technician Interface command that would clear out every ARP entry learned from a specific IP interface. A new command, **clear ip arp prefix/prefix_length**, was added to clear the entries learned on the given subnet.

CR 31861: Compression.

When you run **sync passthru** over MLPPP with compression, and WCP is configured on the PPP interface, several bus errors and tag violations occur.

CR 32070: Dial-on-Demand.

In a configuration where AURP runs over a dial-on-demand line with WCP configured, IP eventually loses connectivity.

CR 32142: IP.

A counter problem causes wfIpInterfaceCacheNetworks to show a larger value than wfIpInterfaceFwdCacheSize. wfIpInterfaceCacheNetworks should never be larger than wfIpInterfaceFwdCacheSize.

CR 32169: Spanning Tree.

The spanning tree algorithm selects the wrong bridge as the root bridge if the difference between two bridge IDs is greater than 0x8001.

CR 32236: Technician Interface.

If you try to save a large configuration file in dynamic mode, the router may have an error which prevents you from saving the file in either Site Manager or the Technician Interface.

CR 33424: BootP.

If there is not enough space in the vendor field of a BootP packet, the following message is logged:

```
2: 09/12/97 14:03:03.410   DEBUG     SLOT  2  BOOTP        Code:  8

Received request on interface 68.224.252.224, inserting subnet mask

Not enough space in vendor field to insert subnet mask
```

CR 32629: DLSw.

This is an enhancement request to support Remote Data Link Correlator. Added wfDlsConnectionEntry.wfDlsConnectionRemoteDLCorr, which contains the Data Link Correlator.

CR 32752: FTP.

During an FTP session, if you interrupt a command by entering Ctrl-C, an orphaned buffer fault may occur and the FTP session terminates.

CR 32779: QLLC.

After you reset the LLC base in a DLS/QLLC environment, you cannot reestablish a session between a PC3270 client and token ring host.

CR 32840: IPX.

In network configurations where a remote router uses group mode frame relay to connect to two different routers, network costing may be set so that one of the local routers connected to the remote router's group mode frame relay will not have an IPX host entry for the remote router. This causes all IPX pings from the remote router to fail. It also causes IPX pings to the remote frame relay interface to fail.

CR 32879: IP.

When you try to configure additional interfaces on a BLN® configured for Host Only Mode, faults occur in *map_rem.c*.

CR 32902: Frame Relay.

The s**how fr stat circ** command displays Drops as Discards and Discards as Drops. The command does display the correct numbers.

CR 33039: DVMRP.

If a neighbor does not send a probe to DUT after the timer is modified, the neighbor does not get timed out as per the new modified timer value (wfDvmrpBaseNeighborTimeout). The neighbor gets timed out with the old timer value. If DUT receives a probe after the timer is modified, the neighbor gets timed out as per the new timer value.

CR 33136: FDDI.

FDDI interface does not recover after receiving PC trace message with external bypass switch.

CR 33353: Frame Relay.

Source route bridging will stop forwarding packets when you dynamically change hybrid mode on a frame relay permanent virtual circuit (PVC). To correct the condition, you must reset the sync interface.

CR 33408: IP.

This is an enhancement request to add a global parameter that causes the router to disregard packets sent to an address that the local router knows is a broadcast address. Added a new attribute to IP Base MIB called wfIpBaseDirectedBcastEnable which should be set to Disabled to turn off directed broadcasts.

CR 33453: LAPB.

LAPB retransmits already acknowledged X.25 packets, causing the X.25 switch on the other side to reset the LAPB session between the X.25 switch and the router. This causes X.25 virtual circuits to be reset and IP circuits over those virtual circuits to come down.

CR 33566: ISDN PRI.

When log messages are written to the log, an exception vector 3 - address error may occur because of a corrupted stack.

CR 33577: IP.

A condition exists in all revisions of code where IP_BARP will consume all buffers on a slot if an external device is trying to reach nonexistent but valid host addresses on a subnet.

A new MIB attribute, wfIpBaseArpBufLimitPrcnt, was added to wfIpBase to specify the percentage of total buffers that can be used by IP_BARP for buffer saving. To monitor this buffer activity, a new IP command, **ip arp_buf**, was added.

CR 33604: IP.

The router stops forwarding ASB packets out an interface after you make a dynamic change to an interface that has the same natural IP network configured as that interface.

CR 33634: IP.

The hog buf in the IP Routing Table Manager can cause the slot to run out of buffers, thereby causing other gates to error on the same slot.

CR 33696: FRAD.

When you configure DLSw in dynamic configuration mode, changing the secondary (HostFRAD) point-to-point or multidrop local device to primary causes all sessions on the port to fail.

CR 34023: DLSw.

When a frame relay link breaks or the FEP fails, the router continues to poll the controller. This prevents the customer from configuring another FEP to call the IPLS.

CR 34159: IP.

A router faults with a watchdog restart when it receives an IP frame that contains a TTL set to 1, IP options of 00 (no options), and 3 bytes of padding to terminate the IP header.

CR 34226: IP.

When you enable the IP Extended Filter Support parameter (wfIpBase.20.0), filters that forward to the next-hop address do not work correctly, resulting in an error.

CR 34254: DLSw.

The log message for a negative CAPx message shows an offset of 0 for certain CAPx errors.

CR 34258: IP.

This is an enhancement request provide the ability to display the total number of IP routes per slot for all slots. Use the command **ip routes -O -s#** (where # is the slot number). If you do not enter a slot number, all slots are displayed.

CR 34264: DLSw.

In an environment using DLSw 1795 with SDLC PU type 2.0 attached devices, when one router sends a flow control reset to another router, the second router still sends one more frame. The first router receives the packet and issues a Halt-DL.

CR 34272: Technician Interface.

This is an enhancement request to increase the severity level of the message `tf_validate: header size invalid, Object.1.18.3.5.1.4.3.1, Instance 29.1.1` to WARNING to indicate that the filter no longer operates correctly.

CR 34298: Technician Interface.

If you telnet to a circuitless IP address on an ARE and run various Technician Interface processes, VBM errors may occur.

CR 34322: TCP.

TCP retransmit-time-out value (RTO) is set to wfTcpRtoMax regardless of actual RTT (even if the actual RTT is short). If wfTcpRtoMax is the default (4 minutes), traffic over TCP (for example, DLS) suddenly stops for 4 minutes.

CR 34416: PPP/Multilink.

This is an enhancement request to change the fragmentation algorithm to require that frames larger than the configured fragment size be fragmented.

CR 34423: X.25.

When a router recovers from congestion, it sends an X.25 RNR packet, but may fail to generate an X.25 RR packet because it is waiting for another part of a fragmented packet.

CR 34471: DLSw.

Performing MIB gets on wfLlcLinkEntry does not show all instances. For example, if you configure DLSw on 2 slots, bring up DLSw connections on both slots, and then enter **g wfLlcLinkEntry.3**, only one circuit is displayed.

CR 34602: DLSw.

A bus error may occur after you delete an X.25 circuit on a client router while two QLLC sessions are active. The bus error also terminates operation of the second circuit on the slot.

CR 34653: DLSw.

A bus error occurs when you boot a BLN router with a variety of DLS configurations.

CR 34660: DLSw.

If you have DLS peers pointing to each other, and one is of type UDP or UNKNOWN and the other is RFC 1795 or RFC 1434, the router with the higher revision will fail to back down to the RFC 1795 router.

CR 34678: DLSw.

When a router receives an SSP Netbios_NQ_ex, it logs it as a CANREACH_ex.

CR 34682: LLC.

LLC2 traffic filter configuration does not work properly when you define a specific range for DSAP or SSAP values. The fact that a RIF field is present is not taken into account when applying the filter to the packet.

CR 34684: APPN.

APPN over LANE does not work.When a router sends a test poll to a second router, the second router does not recognize the destination MAC address and does not forward the packet to APPN. The MAC override should not just change the ESI portion of the NSAP address, but should also change the actual hardware MAC address.

CR 34719: IP.

IP will not install BGP routes when the BGP NEXT_HOP has an unnumbered link as its next hop.

CR 34730: SNMP.

The *WFTRAPS.asn* file shipped with Site Manager needs to be up-to-date with the current image version and the traps it supports. Currently, some of the events are missing.

CR 34738: DLSw.

When you disable DLSw on a router, SDLC Link Stations remain up and continue to poll indefinitely.

CR 34740: Token Ring.

This is an enhancement request to increase the severity of following log message from DEBUG to either INFO or WARNING.

```
#  188: 07/10/97 05:06:05.292  DEBUG  SLOT  3 TOKEN_RING  Code:  26

Connector MAU2 open error, phase=3 error=8.
```

This message indicates that a serious event has occurred -- one that may prevent access to a token ring to a router. The phase and error codes tell you what is halting the access.

CR 34746: QLLC.

A bus error occurs after X.25 calls are cleared several times.

CR 34753: ANH.

After you boot an ANH router using *ti.cfg*, all partition and link LEDs remain on, even though the router does not have an Ethernet interface configured. The lights do not go out until you run the *install* script and select Ethernet as the driver type.

CR 34776: ATM.

An orphan buffer FAULT may occur in an environment where the ATM switch is frequently closing active ATM data virtual circuits.

CR 34868: Translation Bridge.

When a source routing traffic filter is applied to a packet, the router drops the packet destined for the source routing interfaces, but does not drop the packet destined for learning bridge interfaces.

CR 34908: DECnet.

After you enable a DECnet router on an Ethernet VLAN, a VBM error occurs on a router that is attached to the Ethernet VLAN via ATM.

CR 34922: PPP.

After you enable wfPppLineEntry.wfPppLineRfc1661Compliance, the value for wfIpIntfStatsEntry.wfIpIntfStatsMaxInfo does not change. This results in wfIpIntfStatsEntry.wfIpIntfStatsMaxInfo having a larger value than wfPppLineEntry.wfPppLineMru. To change the value for wfIpIntfStatsEntry.wfIpIntfStatsMaxInfo, you must either reboot the router or reset the slot. This fix applies to only non-dial services lines.

CR 34948: DLSw.

The log message `SSP rcv command in TCP local, 14` should be changed to `NetBIOS DATAFRAME Rcv` to be more intuitive to the users reading the log.

CR 34959: DLSw.

Remote DLSw clients do not reestablish a connection to the host after a network disruption.

CR 34988: OSPF.

Bouncing OSPF on an Area Border Router with several point-to-point OSPF nbrs may result in a bus error in OSPF.

CR 35041: IP.

In BayRS Version 12.00 or greater, ASB (all subnet broadcast) does not work in ISP mode.

CR 35116: IPEX.

IPEX in gateway mode will not accept new TCP connection requests for sessions where the TCP peer detected a TCP Open timeout (that is, the router was too slow to accept the request to open). IPEX must be able to recover from unaccepted TCP Accepts.

CR 35129: X.25 Gateway.

If you bring down a large number of sessions by killing the server process, a bus error occurs in the X.25 gateway.

CR 35132: DLSw.

After a router receives an LLC XID frame, the router may not transmit a CANUREACH_cs message, which causes the router connections not to come up.

CR 35136: MIB.

When you issue the **l -i wfMod** command, a bus error occurs. Occasionally, this bus error triggers a GAME restart.

CR 35143: DLSw.

If a NetBIOS client attempts to connect to an Ethernet LANE server or a token ring LANE server, the router terminates operation.

CR 35177: DLSw.

BayRS is not fully compliant with RFC 1434 or RFC 1795 when operating with two half-duplex TCP connections.

CR 35204: DLSw.

A bus error may occur in TCP when IP is bounced on a DLSw router.

CR 35268: DLSw.

When the router receives a multicast SSP NETBIOS_NQ_ex, the ARE experiences several errors, including an exception vector 5 - VBM error.

CR 35328: ARE.

When you use IP traffic filters in ISP mode with the action set to Accept, a bus error occurs if the filter is on an ATM ARE board.

CR 35361: IP.

A bus error may occur when you delete an access policy in the BCC if it was also created in the BCC.

CR 35414: IP.

In a multiline setup with three or more lines, if one of the lines goes down, the router may fail to resolve the far-end host address via ARP.

CR 35428: DLSw.

When you run NetBIOS over DLSw Version 2.0, a panic may occur in *dls_utils.c* as a result of a race condition when establishing connections.

CR 35447: IP.

The router intermittently returns a `Fragmentation Needed but DF set - ICMP Destination Unreachable` message with an incorrect Next-Hop MTU at the end of the ICMP header (low-order 16 bits).

CR 35494: APPN.

When you transfer an APPN topology from one router to another, the topology may not transfer completely.

CR 35502: APPN.

When you activate an APPN link station, a fault occurs because a buffer is freed incorrectly.

CR 35507: PPP.

If you have two routers connected via leased line and PPP using CHAP, and the CHAP timer is set to 0 on one router and to 60 on the other, the router with the timer set to 0 (the receiver) leaks memory. Eventually, that router runs out of memory and restarts.

CR 35523: ISDN.

A bus error occurs in a server one-charge call ID configuration when the router (callback server) is going to set up the call.

CR 35525: DLSw.

If you boot a router that has DLSw Protocol Priority globally enabled and there is an ARE in the router, an exception vector-2 MCP may occur.

CR 35568: Switched Services.

When you use a dial-on-demand asynchronous circuit, you can only establish a connection twice. The third time you try to connect, you cannot ping across the dial-on-demand line.

CR 35571: DLSw.

A router cannot establish a DLSw session if that router has two peers that are terminated on an FDDI port.

CR 35611: BGP.

A VBM error may occur if BGP adds a new route while running on an ARE.

CR 35649/35650: DVMRP.

This is an enhancement request to add a log message indicating that the state of a DVMRP circuit has changed.

CR 35675: IPEX.

When you run a large number of IPEX sessions, some sessions stop passing data after several hours (10 to 15). The more hours IPEX is running, the more sessions stop passing data. The log shows no messages other than clock updates. Statistics show that all X.25, IPEX, and TCP sessions are still in active states.

CR 35685: IP.

When you use a regular expression (for example, **^((123 | 1247 | 2447 | 5432))+ &**) in either BGP policy or **ip bgp_routes -R**, IP returns more matches than expected because the regular expression code incorrectly expands the |.

CR 35721: IPEX.

If the IPEX tcp_accept call fails, the IPEX session is not cleaned up. This causes IPEX sessions to remain in the TCPUP state.

CR 35798: BGP.

If you have multiple BGP connections to the same router and the BGP Collision Detect parameter is set to Disable, the router drops one of the connections and logs a message stating that the connection was dropped because one exists.

CR 35878: DLSw.

DLSw interoperability fails with Cisco 11.3 and IBM routers running RFC 2166.

CR 35887: OSPF.

When you use an OSPF Announce Policy filter to aggregate a range of external networks, the aggregated LSA may constantly refresh if a network within the range is unstable.

CR 35893: IP.

A router configured in ISP mode experiences a bus error within a few minutes following a reboot operation. This happens before BGP imports the full routing table.

CR 35911: OSPF.

An AS External Route may fail to be installed into a routing table if a more specific route with the same address exists. For example, 10.4.0.0/255.252.0.0 would fail to install if 10.4.0.0/255.255.255.0 existed.

CR 35935: DLSw.

When you disconnect a token ring interface, a memory leak occurs and the router slot faults.

CR 35992: ARE.

When an LE_ARP request is sent to an ARE, and the request is for the Group LAN ID of the source route bridges in the network, the ARE fails to respond. Note that the router will now respond to the LE_ARP; however, the network should be designed so that only one Bay Networks router will receive and respond to the LE_ARP that is sent.

CR 36052: OSPF.

A problem exists in OSPF where under certain configurations, it will summarize a summary advertisement that is based on a stub network that is down. When the stub network goes down, OSPF fails to flush the summary generated based on the stub.

CR 71080: IP.

IP traffic filter sends a message to the router log even if there is a match on another traffic filter higher in the list.

CR 71085: OSPF.

In an Autonomous System Border Router (ASBR), when you create a new IP interface, it is immediately advertised as a type 5 external by OSPF. Later, when OSPF is configured on that interface, it now becomes a type 1 or 2 and is advertised as such. However, OSPF does not flush out the old type 5 that was generated.

CR 71443: IPX.

A problem occurs in which the router experiences a bus error when a host sends a RIP request or SAP request using a source socket of 9001 (NLSP).

CR 71475: ISDN.

For an ISDN leased line media type, the inter-frame fill pattern should be 7E instead of FF.

CR 71634: IPEX.

When IPEX in gateway mode is operational, the router exceeds buffer space when many TCP sessions are torn down because the TCP server is disabled. When you restart the server, the IPEX/TCP sessions do not re-establish.

CR 71703: IPEX.

When you request IPEX configured in gateway mode to bring up many TCP sessions, the router takes too long to process all the TCP open requests, causing the peer to time out some of the open requests.

CR 71738: IP.

A configuration with multiple BGP regular expressions may cause the log to be filled with `Truncating regular expression` warning messages. However, the processing of the regular expression was not affected.

CR 71739: IP.

The **ip bgp_routes -N** command may display routes that are not really being announced.

CR 71767: AppleTalk.

A problem occurs in AppleTalk in which an ARE interface can experience VBM errors. This problem can occur in an environment in which there is a variety of extended networks and non-extended networks.

CR 71779: IPX.

IPX route filters fail to work properly if you configure multiple filters on a circuit, each with a different priority. In this case, only the first filter (first one created and highest priority) is matched.

CR 72074: X.25.

If X.25 receives a disconnect request from the local interface and then receives a disconnect from the remote interface through IPEX, the VC may remain in an operational state and never be cleared.

CR 72526: IPEX.

IPEX in gateway mode incorrectly accepts new TCP connection requests before the previous session was completely terminated, causing the IPEX session to hang.

Site Manager Software Version 6.02 Fixed Anomalies

Bay Networks has fixed the following anomalies in Site Manager Software Version 6.02.

==========

Site Manager Software Version 6.02 is a post-6.00 revision. This version is backward compatible and supports the following router software versions:

12.02

12.01

12.00

11.02

11.01

11.00

10.01

==========

CR 78926: SDLC.

After you change the DLSw mode on the SDLC link from Secondary to Primary, the configuration becomes corrupted and causes SDLC to continuously issue bus errors until the slot resets.

CR 79837: IPEX/X.25.

This is an enhancement request to expand the range of TCP port numbers available for use by IPEX/X25 gateway when configuring the local TCP port in mapping entries. The current range allowed is 12304 to 16399. The range should be 10256 to 16399 to allow for 768 mappings to exist on up to 8 slots of a router (for a total of 6144 sessions per router).

CR 71031: BGP.

In order for BGP routes to be exported to the OSPF link state database, the BGP Intra-AS parameter must be set to Disabled. By default, this parameter is set to Enabled. If you disable this parameter dynamically, Site Manager generates multiple bus errors and a watchdog.

CR 32979: APPN.

When you configure the APPN protocol and you enter a local node name, a core dump occurs.

CR 78156: Source Route Bridge.

When you configure a sync interface for source route bridging, the Source Routing Interfaces window from the Protocols pull-down menu option on the Frame Relay Service List window shows all 0s for the sync interface.

CR 78538: Router Redundancy.

When you configure the Automatic Role Switching parameter from the Router Redundancy Group Global window, the Values button shows only two options: Manual and Auto. According to the Help window and to the documentation, four options are available: Manual, Auto, Switch on Failure, and One Shot Auto.

CR 78722: IPX.

If you enter a valid DLCI in the IPX adjacent host definition, Site Manager displays an error message, indicating that you have entered an incorrect number range or format.

CR 75561: IP.

When you reorder a small traffic filter, in ascending or descending order, past a large traffic filter with many IP addresses within the same filter, a memory fault condition occurs on the router. In some cases, Site Manager unloads IP from the slot.

CR 75236: MCT.

Accessing circuit information for an MCT1 causes Site Manager to abort with the following error: `The Configuration" module completed abnormally. (E1701).`

CR 35695: SNMP.

When you attempt to delete an SNMP community, the message `SNMP Set Error` appears. When you press OK or Cancel to remove the message, the message reappears.

CR 75254: SNMP.

When you click on OK from the Edit Adapter Module 2, 56/64K DUS CSU Parameters window, Site Manager sets the attribute wfSyncExternalClkSpeed to the value determined by the Option Mode parameter, even if the attribute's value has not changed.

CR 76000: ISDN.

When you configure an MCT-1 port for PRI and you enable RFC 1661 compliance, if you change the MRU size, the information message `Please make sure that the SYNC MTU is >= PPP MRU + 56 bytes` appears for each channel on the MCT-1 port. The message should only appear once.

CR 73309: BGP.

Site Manager does not allow you to change the value for the Route Preference parameter in a BGP4 accept policy.

CR 75049: IP.

When you delete BGP-3 from a configuration, Site Manager deletes all the IBGP peers.

CR 75303: X.25.

When you add an X.25/PTOP line, the Connection ID parameter defaults to 0. The range of valid values is from 1 to 255.

CR 75341: Sync.

When you select the Values button for the Sync B Channel Override parameter, the message `Sorry, No additional information available` appears. The valid values are BCHANNEL1, BCHANNEL2, Default, and FLOATINGB.

CR 72050: Traffic Filters.

When you delete a traffic filter in dynamic or remote mode, Site Manager does not remove the filter from the list. In local mode, Site Manager removes the filter when you save the configuration file.

CR 75894: Protocol Priority.

When you apply a new Protocol Priority outbound filter, Configuration Manager faults and then terminates. The fault occurs on the PC only.

CR 28400: Router Files Manager.

If you enter an invalid community name in the Router Files Manager window, Site Manager displays the error message `Unable to reach Router`. When you click on OK, the same message appears again.

CR 72781: FireWall.

The FireWall product was introduced in 11.02/Rev 2. When you use Site Manager to connect to a router that is running a release earlier than 11.02, the FireWall menu should be unavailable.

CR 71674: APPN.

If you use Site Manager to configure an APPN interface over frame relay using source routing, and you add an Adjacent Link Station, Site Manager incorrectly sets the MIB attribute wfAppnNodeDlcType to 3 (transparent bridging). The correct setting for this attribute is 2 (source routing).

CR 72630: Token Ring.

When you attempt to configure traps on a token ring interface, that interface is not available in "Available Entities."

CR 73066: TCP.

The delete confirmation windows for Telnet server and Telnet client contain a typo.

CR 71347: DLSw.

When you configure an 802.5 service record for DLS/LLC/SRB, Site Manager incorrectly sets the DLS DLC type (wfDlsInterfaceEntry.wfDlsInterfaceDlcType) to 3 (learning bridge); the DLS DLC type should be set to 2 (source route).

CR 36017: Image Builder.

If you are using Image Builder in Site Manager Software Version 6.01 to modify a Router Software Version 11.03 router image, the following error message appears: `The cross-referenced file is not up-to-date relative to the image stamp.`

CR 72567: DLSw.

When you configure DLSw, Site Manager sets the TCP max window size to 1 (wfTcp.18.0 = 1). The value should be set to the same value for which wfDlsTcpWindowSize is configured.

CR 71137: DLSw.

When you add DLSw to an X.25/QLLC service record, Site Manager displays the following error message: `Data entered for '(null)' is inconsistent with the packet level. Do you want the related packet/service record attributes set correctly?` When you click on the Apply button, Site Manager core dumps or GPFs.

CR 35781: DLSw.

If the router is running pre-BayRS 12.00 router code, the DLSw Backup Peer MIB attributes on the DLSw Peer Configuration window are incorrect.

CR 31321: DLSw.

If you configure a local device with maxdata on the DLSw local device window, when you exit the window, an error message appears, warning you that the maxdata is larger then the sync MTU. This happens only in dynamic mode.

CR 34913: Source Route Bridge.

After you configure source route bridge on a dial-on-demand circuit or an ATM service record, the source route interface window displays zeroes in all fields for that circuit.

CR 35239: X.25.

When you configure X.25/QLLC Maps, Site Manager leaves the Generate XID field empty. To save the window, you must enter Enable in the Generate XID field. However, Site Manager incorrectly sets the MIB entry for this field to a number between 15-20, and the configuration does not work. To correct the problem, set the MIB attribute for the Generate XID field to 1.

CR 35692: SNMP.

When you run Configuration Manager in dynamic mode, the wfProtocols.wfIPROTOLoad gets set to the value to which it is already set. However, the set does not affect service.

CR 72071: FDDI.

When you change a slot containing an FDDI module to Empty Slot, Site Manager does not delete the following enhanced FDDI MIB objects from the configuration file: wfFddiSmtExtEntry, wfFddiSmtActionEntry, wfFddiMacExtEntry, wfFddiPathExtEntry, wfFddiPortExtEntry, and wfFddiPortActionEntry.

CR 35797: BGP.

Although the Multihop EBGP Connection parameter is set to Enabled, you cannot configure BGP peers that are not on the same subnet.

CR 34872: PPP.

SYNC MTU must be at least 56 bytes greater than PPPMRU.

CR 35580: LLC2 traffic filters.

Site Manager lets you create LLC2 traffic filters under the wrong circuit number. If you create an LLC2 traffic filter by selecting LLC Circuit > LLC2 Circuit and then Protocols > LLC2 Traffic filters, the filter will not work because Site Manager uses a circuit number that is different from the number assigned to this interface.

CR 30906: IP.

A problem exists when you apply a template to a circuit that has one IP source address range, 22 IP destination address ranges, and at least one TCP destination port. When this template is applied to a circuit, it shows up in two fragments. Neither fragment has a circuit number or IP address; both fragments are inactive.

CR 35936: IP.

When you use a circuitless IP address with an instance number of 1 (under wfCircuitNameEntry), Site Manager can cause the router to unload and reload certain protocols.

CR 33589: IPX.

When you delete IPX from a WAN interface (e.g., frame relay or PPP), Site Manager does not remove the IPX circuit instance completely.

CR 34024: BOT.

This is an enhancement request to enable the Bisync protocol to support more leading SYNC characters. Currently, the BISYNC code is hardcoded for 2 leading SYNC characters, and should be hardcoded for 7 SYNC characters. The router software code requires configurable leading SYNC characters in order to interoperate.

CR 35899: BGP.

When you create a BGP peer for a circuitless IP address, invalid and/or multiple instances of wfCircuitNameEntry are created.

CR 35918: Switched Services.

When you delete a dial-on-demand schedule entry, the following error message appears: `Function was not found (xref_standby_tod_delete).` This message occurs only when you use Site Manager to configure an 11.02 or an 11.01 MIB attribute.

No CR: Dial on Demand.

If you configure scheduled dial-on-demand, and you accept the default of 2400 for the End of Time parameter, an error occurs.